CSAR / CHAT CONTROL
Infrastructure Vulnerability Assessment
Basato su report governativi, leak verificati e analisi crittografiche pubbliche

Luglio 2026

1. L'ARCHITETTURA CSAR

Il regolamento CSAR, che tutti chiamano Chat Control, impone a ogni piattaforma di messaggistica di scansionare foto, video e link direttamente sul dispositivo dell'utente, prima che vengano crittografati. Non è un controllo a valle: è un algoritmo che si installa nel tuo telefono e guarda cosa condividi.

Tutto quello che viene segnalato finisce all'EU Centre, che molto probabilmente avrà sede all'Aia: un unico nodo centrale dove confluiscono miliardi di segnalazioni da tutte le piattaforme, per essere filtrate e smistate alle forze di polizia nazionali.

Il punto non è se funziona. Il punto è che l'architettura stessa è una vulnerabilità: una backdoor crittografica generalizzata, un honeypot centralizzato, un vettore di attacco già pronto per chiunque abbia i mezzi per sfruttarlo, servizi di intelligence ostili, criminalità organizzata, gruppi APT

2. LA FINE DELLA CRITTOGRAFIA END-TO-END

Più di trecento esperti internazionali di crittografia, tra cui Bruce Schneier e Ross Anderson, nomi che pesano, hanno pubblicato analisi tecniche in cui dimostrano che il Client-Side Scanning e la crittografia end-to-end non possono coesistere. Sono mutuamente esclusivi.

Il motivo è semplice: per scansionare un messaggio prima che venga crittografato, devi intercettarlo quando è ancora in chiaro. Significa che nel dispositivo esiste un punto in cui il contenuto è leggibile. E se è leggibile per un algoritmo di rilevamento, è leggibile per chiunque riesca a compromettere quell'algoritmo.

La differenza tra un client di scansione e uno spyware di stato è zero. Entrambi intercettano, analizzano ed esfiltrano dati. La backdoor non è un bug: è il progetto.

3. HASH, COLLISIONI E AVVELENAMENTO

Il sistema si basa su hash percettivi, principalmente PhotoDNA di Microsoft e PDQ. Il funzionamento è questo: ogni immagine sul tuo dispositivo viene ridotta a una stringa (hash) e confrontata con un database di hash "illegali". Se matcha, scatta la segnalazione.

Il problema è che i sistemi di hashing percettivo sono vulnerabili agli adversarial examples. Modificando pixel invisibili a occhio nudo in un'immagine innocua, è possibile generare lo stesso hash di un'immagine illegale presente nel database.

Questo significa che chiunque abbia accesso al sistema può incastrare chiunque. Prendi una foto di un attivista, modifichi tre pixel, e improvvisamente quell'hash corrisponde a materiale pedopornografico. Parte la segnalazione. L'attivista finisce sotto indagine. E nel frattempo l'EU Centre, che raccoglie tutto in un unico posto, diventa il bersaglio perfetto per esfiltrazioni massive e spionaggio industriale. È l'opposto di quello che qualsiasi esperto di sicurezza chiamerebbe Zero Trust.

4. I DATI CHE GIÀ ABBIAMO

Non dobbiamo immaginare cosa succederà. Possiamo guardare cosa succede adesso, nei paesi dove sistemi simili sono già attivi tramite i report NCMEC.

In Svizzera, la polizia federale (Fedpol) dichiara che l'ottanta percento delle segnalazioni automatiche ricevute è completamente irrilevante dal punto di vista penale. Falsi positivi. Il risultato è che gli investigatori passano il tempo a smaltire notifiche inutili mentre i casi veri aspettano.

In Germania, il BKA riporta che tra il quaranta e il cinquanta percento dei report non porta ad alcuna indagine perché semplicemente non c'è reato. Cittadini innocenti vengono spiati. La loro privacy violata. E in cambio non si ottiene nulla.

I dati NCMEC mostrano un'altra cosa: oltre il quaranta percento delle segnalazioni coinvolge minori che fanno sexting, ragazzi che si scambiano foto consensuali. L'algoritmo non distingue. E questi minori finiscono automaticamente nei database delle forze dell'ordine. Criminalizzati da un software.

5. LA PARTE CHE NON TI RACCONTANO

Durante i negoziati, un documento interno del Consiglio dell'Unione Europea è trapelato ed è stato pubblicato dall'eurodeputato Patrick Breyer. Il documento mostrava che il Consiglio stava discutendo una clausola per esentare dalla scansione agenzie governative, polizia, forze armate e servizi di intelligence nazionali.

Rileggiamolo: gli Stati membri vogliono essere sicuri che i loro segreti non passino attraverso il sistema che vogliono imporre a te. Se il sistema è troppo insicuro per i segreti di Stato, perché dovrebbe essere sicuro per i tuoi? E non è solo una questione di buonsenso. Il Garante Europeo della Protezione dei Dati e il Comitato Europeo per la Protezione dei Dati hanno pubblicato pareri congiunti in cui dichiarano che la normativa viola palesemente la Carta dei diritti fondamentali dell'Unione Europea. Parole loro: l'infrastruttura è legalmente e tecnicamente insostenibile.

6. IL QUADRO COMPLETO: NON È SOLO CHAT CONTROL

Sarebbe già abbastanza grave se fosse una legge isolata. Ma non lo è.

L'Unione Europea sta costruendo tre pilastri normativi che, messi insieme, producono qualcosa di molto più ambizioso di un sistema anti-abuso. Producono un profilo digitale totale di ogni cittadino.

Il primo pilastro è l'identità digitale europea, il regolamento eIDAS 2.0. Ogni cittadino riceve un wallet digitale obbligatorio che lega la sua identità reale in modo univoco e permanente a ogni interazione online. Non esiste più l'anonimato. Ogni login, ogni accesso, ogni servizio: tutto è ricondotto a te, con nome e cognome.

Il secondo pilastro è l'euro digitale. La Banca Centrale Europea sta sviluppando una moneta digitale con transazioni registrate. Ogni pagamento è tracciabile, collegato all'identità digitale, archiviato in modo permanente. Il contante, l'ultimo rifugio di privacy finanziaria, diventa progressivamente inutilizzabile.

Il terzo pilastro è il Chat Control. Scansione obbligatoria di ogni comunicazione privata. Il contenuto delle tue conversazioni è accessibile, analizzabile, segnalabile.

Mettili insieme. Lo Stato sa chi sei (eIDAS), sa cosa dici (CSAR), sa cosa compri e a chi (digital euro). Non serve più un regime autoritario che ti metta in prigione. Basta che il sistema sappia tutto di te. Il resto, cosa puoi fare, cosa puoi comprare, cosa puoi dire, lo decide l'algoritmo.

Questa architettura abilita propaganda personalizzata basata sul tuo comportamento reale, scoring sociale automatizzato, ricatto informativo su qualsiasi cosa tu voglia nascondere, ed esclusione digitale per chi rifiuta il wallet. Nessuno scenario distopico: eIDAS è già in vigore. L'euro digitale è in fase pilota. CSAR è in trilogo. Quando l'ultimo pilastro sarà operativo, la trasformazione sarà irreversibile. E sarà silenziosa.

7. CONCLUSIONE

L'architettura CSAR non ha bug da correggere. È vulnerabile per come è stata progettata. Qualsiasi implementazione funzionante esporrà le comunicazioni europee a una backdoor crittografica generalizzata, a un collasso operativo per eccesso di falsi positivi, a un

honeypot centralizzato per intelligence ostili e all'avvelenamento selettivo degli hash per colpire bersagli specifici.

Nel quadro più ampio, CSAR è il tassello finale di un sistema integrato che trasforma i cittadini in profili digitali completi, tracciabili, prevedibili, controllabili. Non per colpire "i criminali". Per colpire chiunque.

Se questo documento serve a qualcosa, è a rendere chiaro che non stiamo parlando di una legge sbagliata. Stiamo parlando della fine della privacy come l'abbiamo conosciuta.

FONTI

Fedpol, rapporto interno su segnalazioni automatiche NCMEC
BKA, statistiche investigative sui report di scansione automatica
NCMEC, dati aggregati su segnalazioni e indagini
Consiglio dell'Unione Europea, Working Paper trapelato (pubblicato da Patrick Breyer, MEP)
EDPS / EDPB, pareri pubblici congiunti sulla proposta CSAR
Schneier, Anderson et al., analisi tecnica su Client-Side Scanning e crittografia end-to-end
Regolamento eIDAS 2.0 (EU 2024/1183)
BCE, report fase preparatoria euro digitale (2023-2025)